[ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ]

[Институт ИИБС, Кафедра ИСКТ]

[Шумейко Е.В.]

Основные определения и критерии классификации угроз

Основные определения и критерии классификации угроз

Угроза - это потенциальная возможность определенным образом нарушить информационную безопасность. Попытка реализации *угрозы* называется ***атакой***, а тот, кто предпринимает такую попытку, - ***злоумышленником***. Потенциальные *злоумышленники* называются ***источниками угрозы***.

Чаще всего *угроза* является следствием наличия *уязвимых* мест в защите информационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Основные определения и критерии классификации угроз

Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется ***окном опасности***, ассоциированным с данным *уязвимым* местом. Пока существует *окно опасности*, возможны успешные *атаки* на ИС.

Если речь идет об ошибках в ПО, то *окно опасности* "открывается" с появлением средств использования ошибки и ликвидируется при наложении заплат, ее исправляющих.

Основные определения и критерии классификации угроз

Для большинства *уязвимых* мест *окно опасности* существует сравнительно долго (несколько дней, иногда - недель), поскольку за это время должны произойти следующие события:

- должно стать известно о средствах использования пробела в защите;
- должны быть выпущены соответствующие заплаты;
- заплаты должны быть установлены в защищаемой ИС.

Основные определения и критерии классификации угроз

Мы уже указывали, что новые *уязвимые* места и средства их использования появляются постоянно; это значит, во-первых, что почти всегда существуют окна опасности и, во-вторых, что отслеживание таких окон должно производиться постоянно, а выпуск и наложение заплат - как можно более оперативно.

Отметим, что некоторые *угрозы* нельзя считать следствием каких-то ошибок или просчетов; они существуют в силу самой природы современных ИС. Например, *угроза* отключения электричества или выхода его параметров за допустимые границы существует в силу зависимости аппаратного обеспечения ИС от качественного электропитания.

Основные определения и критерии классификации угроз

Рассмотрим наиболее распространенные *угрозы*, которым подвержены современные информационные системы. Иметь представление о возможных *угрозах*, а также об *уязвимых* местах, которые эти *угрозы* обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности. Слишком много мифов существует в сфере информационных технологий (вспомним все ту же "Проблему 2000"), поэтому незнание в данном случае ведет к перерасходу средств и, что еще хуже, к концентрации ресурсов там, где они не особенно нужны, за счет ослабления действительно *уязвимых* направлений.

Основные определения и критерии классификации угроз

Подчеркнем, что само понятие "*угроза*" в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации *угроз* конфиденциальности может просто не существовать - вся информация считается общедоступной; однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, *угрозы*, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Мы попытаемся взглянуть на предмет с точки зрения типичной (на наш взгляд) организации. Впрочем, многие *угрозы* (например, пожар) опасны для всех.

Основные определения и критерии классификации угроз

Угрозы можно классифицировать по нескольким критериям:

- по аспекту информационной безопасности (доступность, целостность, конфиденциальность), против которого *угрозы* направлены в первую очередь;
- по компонентам информационных систем, на которые *угрозы* нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению *источника угроз* (внутри/вне рассматриваемой ИС)..

Основные определения и критерии классификации угроз

В качестве основного критерия мы будем использовать первый (по аспекту ИБ), привлекая при необходимости остальные.

Наиболее распространенные угрозы доступности

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются *непреднамеренные ошибки* штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы.

Иногда такие ошибки и являются собственно *угрозами* (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают *уязвимые* места, которыми могут воспользоваться *злоумышленники* (таковы обычно ошибки администрирования). По некоторым данным, до 65% потерь - следствие *непреднамеренных ошибок*.

Наиболее распространенные угрозы доступности

Пожары и наводнения не приносят столько бед, сколько безграмотность и небрежность в работе.

Очевидно, самый радикальный способ борьбы с *непреднамеренными ошибками* - максимальная автоматизация и строгий контроль.

Другие *угрозы* доступности классифицируем по компонентам ИС, на которые нацелены *угрозы*:

- *отказ пользователей*;
- *внутренний отказ* информационной системы;
- *отказ поддерживающей инфраструктуры*.

Наиболее распространенные угрозы доступности

Обычно применительно к пользователям рассматриваются следующие *угрозы*:

- нежелание работать с информационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Наиболее распространенные угрозы доступности

Основными источниками *внутренних отказов* являются:

- отступление (случайное или умышленное) от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);
- ошибки при (пере)конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или *повреждение аппаратуры*.

Наиболее распространенные угрозы доступности

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие *угрозы*:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его *угроза*, забастовка и т.п.).

Наиболее распространенные угрозы доступности

Весьма опасны так называемые *"обиженные" сотрудники* - нынешние и бывшие. Как правило, они стремятся нанести вред организации-"обидчику", например:

- испортить оборудование;
- встроить логическую *бомбу*, которая со временем разрушит программы и/или данные;
- удалить данные.

Наиболее распространенные угрозы доступности

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались.
Опасны, разумеется, *стихийные бедствия* и события, воспринимаемые как *стихийные бедствия*,- пожары, наводнения, землетрясения, ураганы. По статистике, на долю огня, воды и тому подобных "*злоумышленников*" (среди которых самый опасный - перебой электропитания) приходится 13% потерь, нанесенных информационным системам.

Некоторые примеры угроз доступности

Угрозы доступности могут выглядеть грубо - как *повреждение* или даже разрушение **оборудования** (в том числе носителей данных). Такое повреждение может вызываться естественными причинами (чаще всего - грозами). К сожалению, находящиеся в массовом использовании источники бесперебойного питания не защищают от мощных кратковременных импульсов, и случаи выгорания оборудования - не редкость.

Некоторые примеры угроз доступности

В принципе, мощный кратковременный импульс, способный разрушить данные на магнитных носителях, можно сгенерировать и искусственным образом - с помощью так называемых высокоэнергетических радиочастотных пушек. Но, наверное, в наших условиях подобную *угрозу* следует все же признать надуманной.

Некоторые примеры угроз доступности

Действительно опасны протечки водопровода и отопительной системы. Часто организации, чтобы сэкономить на арендной плате, снимают помещения в домах старой постройки, делают косметический ремонт, но не меняют ветхие трубы. Автору курса довелось быть свидетелем ситуации, когда прорвало трубу с горячей водой, и системный блок компьютера (это была рабочая станция производства Sun Microsystems) оказался заполнен кипятком. Когда кипяток вылили, а компьютер просушили, он возобновил нормальную работу, но лучше таких опытов не ставить...

Некоторые примеры угроз доступности

Летом, в сильную жару, норовят сломаться кондиционеры, установленные в серверных залах, набитых дорогостоящим оборудованием. В результате значительный ущерб наносится и репутации, и кошельку организации.

Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные носители зачастую хранят небрежно (к этому мы еще вернемся при обсуждении *угроз* конфиденциальности), не обеспечивая их защиту от вредного воздействия окружающей среды. И когда требуется восстановить данные, оказывается, что эти самые носители никак не желают читаться.

Некоторые примеры угроз доступности

Перейдем теперь к *угрозам* доступности, которые будут похитрее засоров канализации. Речь пойдет о программных *атаках* на доступность.

В качестве средства вывода системы из штатного режима эксплуатации может использоваться *агрессивное потребление ресурсов* (обычно - полосы пропускания сетей, вычислительных возможностей процессоров или оперативной памяти). По расположению *источника угрозы* такое **потребление** подразделяется на ***локальное*** и ***удаленное***. При просчетах в конфигурации системы локальная программа способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю.

Некоторые примеры угроз доступности

Простейший пример *удаленного потребления* ресурсов - *атака*, получившая наименование "SYN-наводнение". Она представляет собой попытку переполнить таблицу "полуоткрытых" TCP-соединений сервера (установление соединений начинается, но не заканчивается). Такая *атака* по меньшей мере затрудняет установление новых соединений со стороны легальных пользователей, то есть сервер выглядит как недоступный.

По отношению к *атаке* "Papa Smurf" *уязвимы* сети, воспринимающие ping-пакеты с широковещательными адресами. Ответы на такие пакеты "съедают" полосу пропускания.

Некоторые примеры угроз доступности

Удаленное потребление ресурсов в последнее время проявляется в особенно опасной форме - как скоординированные распределенные *атаки*, когда на сервер с множества разных адресов с максимальной скоростью направляются вполне легальные запросы на соединение и/или обслуживание. Временем начала "моды" на подобные *атаки* можно считать февраль 2000 года, когда жертвами оказались несколько крупнейших систем электронной коммерции (точнее - владельцы и пользователи систем). Отметим, что если имеет место архитектурный просчет в виде разбалансированности между пропускной способностью сети и производительностью сервера, то защититься от распределенных *атак* на доступность крайне трудно.

Некоторые примеры угроз доступности

Для выведения систем из штатного режима эксплуатации могут использоваться *уязвимые* места в виде программных и аппаратных ошибок. Например, известная ошибка в процессоре Pentium I дает возможность локальному пользователю путем выполнения определенной команды "подвесить" компьютер, так что помогает только аппаратный RESET.
Программа "Teardrop" удаленно "подвешивает" компьютеры, эксплуатируя ошибку в сборке фрагментированных IP-пакетов.

Вредоносное программное обеспечение

Одним из опаснейших способов проведения *атак* является внедрение в *атакуемые* системы *вредоносного программного обеспечения*.

Мы выделим следующие грани *вредоносного ПО*:

- вредоносная функция;
- способ распространения;
- внешнее представление.

Вредоносное программное обеспечение

Часть, осуществляющую разрушительную функцию, будем называть ***"бомбой"*** (хотя, возможно, более удачными терминами были бы "заряд" или "боеголовка"). Вообще говоря, спектр вредоносных функций неограничен, поскольку *"бомба"*, как и любая другая программа, может обладать сколь угодно сложной логикой, но обычно *"бомбы"* предназначаются для:

- внедрения другого *вредоносного ПО*;
- получения контроля над *атакуемой* системой;
- *агрессивного потребления ресурсов*;
- изменения или разрушения программ и/или данных.

Вредоносное программное обеспечение

По механизму распространения различают:

- ***вирусы*** - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;
- ***"черви"*** - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации *вируса* требуется запуск зараженной программы).

Вредоносное программное обеспечение

Вирусы обычно распространяются локально, в пределах узла сети; для передачи по сети им требуется внешняя помощь, такая как пересылка зараженного файла. *"Черви"*, напротив, ориентированы в первую очередь на путешествия по сети.

Иногда само распространение *вредоносного ПО* вызывает *агрессивное потребление ресурсов* и, следовательно, является вредоносной функцией. Например, *"черви"* "съедают" полосу пропускания сети и ресурсы почтовых систем. По этой причине для *атак* на доступность они не нуждаются во встраивании специальных *"бомб"*.

Вредоносное программное обеспечение

Вредоносный код, который выглядит как функционально полезная программа, называется *троянским*. Например, обычная программа, будучи пораженной *вирусом*, становится ***троянской***; порой *троянские программы* изготавливают вручную и подсовывают доверчивым пользователям в какой-либо привлекательной упаковке. Отметим, что данные нами определения и приведенная классификация *вредоносного ПО* отличаются от общепринятых. Например, в ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения" содержится следующее определение:

Вредоносное программное обеспечение

"Программный *вирус* - это исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или телекоммуникационных сетях с целью изменить или уничтожить программное обеспечение и/или данные, хранящиеся в автоматизированных системах".
На наш взгляд, подобное определение неудачно, поскольку в нем смешаны функциональные и транспортные аспекты.

Вредоносное программное обеспечение

Окно опасности для *вредоносного ПО* появляется с выпуском новой разновидности *"бомб"*, *вирусов* и/или *"червей"* и перестает существовать с обновлением базы данных антивирусных программ и наложением других необходимых заплат.

По традиции из всего *вредоносного ПО* наибольшее внимание общественности приходится на долю *вирусов*. Однако до марта 1999 года с полным правом можно было утверждать, что "несмотря на экспоненциальный рост числа известных *вирусов*, аналогичного роста количества инцидентов, вызванных ими, не зарегистрировано. Соблюдение несложных правил "компьютерной гигиены" практически сводит риск заражения к нулю. Там, где работают, а не играют, число зараженных компьютеров составляет лишь доли процента".

Вредоносное программное обеспечение

В марте 1999 года, с появлением *вируса* "Melissa", ситуация кардинальным образом изменилась. "Melissa" - это макро*вирус* для файлов MS-Word, распространяющийся посредством электронной почты в присоединенных файлах. Когда такой (зараженный) присоединенный файл открывают, он рассылает свои копии по первым 50 адресам из адресной книги Microsoft Outlook. В результате почтовые серверы подвергаются *атаке* на доступность.

Вредоносное программное обеспечение

В данном случае нам хотелось бы отметить два момента.

1. Как уже говорилось, пассивные объекты отходят в прошлое; так называемое ***активное содержимое*** становится нормой. Файлы, которые по всем признакам должны были бы относиться к данным (например, документы в форматах MS-Word или Postscript, тексты почтовых сообщений), способны содержать интерпретируемые компоненты, которые могут запускаться неявным образом при открытии файла. Как и всякое в целом прогрессивное явление, такое "повышение активности данных" имеет свою оборотную сторону (в рассматриваемом случае - отставание в разработке механизмов безопасности и ошибки в их реализации).

Вредоносное программное обеспечение

Обычные пользователи еще не скоро научатся применять интерпретируемые компоненты "в мирных целях" (или хотя бы узнают об их существовании), а перед *злоумышленниками* открылось по существу неограниченное поле деятельности. Как ни банально это звучит, но если для стрельбы по воробьям выкатывается пушка, то пострадает в основном стреляющий.

Вредоносное программное обеспечение

2. Интеграция разных сервисов, наличие среди них сетевых, всеобщая связность многократно увеличивают потенциал для *атак* на доступность, облегчают распространение *вредоносного ПО* (*вирус* "Melissa" - классический тому пример). Образно говоря, многие информационные системы, если не принять защитных мер, оказываются "в одной лодке" (точнее - в корабле без переборок), так что достаточно одной пробоины, чтобы "лодка" тут же пошла ко дну.

Вредоносное программное обеспечение

Как это часто бывает, вслед за "Melissa" появилась на свет целая серия *вирусов*, *"червей"* и их комбинаций: "Explorer.zip" (июнь 1999), "Bubble Boy" (ноябрь 1999), "ILOVEYOU" (май 2000) и т.д. Не то что бы от них был особенно большой ущерб, но общественный резонанс они вызвали немалый.

Вредоносное программное обеспечение

Активное содержимое, помимо интерпретируемых компонентов документов и других файлов данных, имеет еще одно популярное обличье - так называемые ***мобильные агенты***. Это программы, которые загружаются на другие компьютеры и там выполняются. Наиболее известные примеры *мобильных агентов* - Java-апплеты, загружаемые на пользовательский компьютер и интерпретируемые Internet-навигаторами. Оказалось, что разработать для них модель безопасности, оставляющую достаточно возможностей для полезных действий, не так-то просто; еще сложнее реализовать такую модель без ошибок.

Вредоносное программное обеспечение

В августе 1999 года стали известны недочеты в реализации технологий ActiveX и Java в рамках Microsoft Internet Explorer, которые давали возможность размещать на Web-серверах вредоносные апплеты, позволяющие получать полный контроль над системой-визитером.

Вредоносное программное обеспечение

Для внедрения *"бомб"* часто используются ошибки типа *"переполнение буфера"*, когда программа, работая с областью памяти, выходит за границы допустимого и записывает в нужные *злоумышленнику* места определенные данные. Так действовал еще в 1988 году знаменитый *"червь* Морриса"; в июне 1999 года хакеры нашли способ использовать аналогичный метод по отношению к Microsoft Internet Information Server (IIS), чтобы получить контроль над Web-сервером. *Окно опасности* охватило сразу около полутора миллионов серверных систем...

Вредоносное программное обеспечение

Не забыты современными *злоумышленниками* и испытанные *троянские программы*. Например, *"троянцы"* Back Orifice и Netbus позволяют получить контроль над пользовательскими системами с различными вариантами MS-Windows.

Таким образом, действие *вредоносного ПО* может быть направлено не только против доступности, но и против других основных аспектов информационной безопасности.

Основные угрозы целостности

На втором месте по размерам ущерба (после *непреднамеренных ошибок* и упущений) стоят *кражи* и *подлоги*. По данным газеты USA Today, еще в 1992 году в результате подобных противоправных действий с использованием персональных компьютеров американским организациям был нанесен общий ущерб в размере 882 миллионов долларов. Можно предположить, что реальный ущерб был намного больше, поскольку многие организации по понятным причинам скрывают такие инциденты; не вызывает сомнений, что в наши дни ущерб от такого рода действий вырос многократно.

Основные угрозы целостности

В большинстве случаев виновниками оказывались штатные сотрудники организаций, отлично знакомые с режимом работы и мерами защиты. Это еще раз подтверждает опасность внутренних *угроз*, хотя говорят и пишут о них значительно меньше, чем о внешних.
Ранее мы проводили различие между *статической* и *динамической целостностью*. С целью нарушения *статической целостности злоумышленник* (как правило, штатный сотрудник) может:

- ввести неверные данные;
- изменить данные.

Основные угрозы целостности

Иногда изменяются содержательные данные, иногда - служебная информация. Показательный случай нарушения целостности имел место в 1996 году. Служащая Oracle (личный секретарь вице-президента) предъявила судебный иск, обвиняя президента корпорации в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина привела электронное письмо, якобы отправленное ее начальником президенту. Содержание письма для нас сейчас не важно; важно время отправки. Дело в том, что вице-президент предъявил, в свою очередь, файл с регистрационной информацией компании сотовой связи, из которого явствовало, что в указанное время он разговаривал по мобильному телефону, находясь вдалеке от своего рабочего места.

Основные угрозы целостности

Таким образом, в суде состоялось противостояние "файл против файла". Очевидно, один из них был фальсифицирован или изменен, то есть была нарушена его целостность. Суд решил, что подделали электронное письмо (секретарша знала пароль вице-президента, поскольку ей было поручено его менять), и иск был отвергнут...

Основные угрозы целостности

(Теоретически возможно, что оба фигурировавших на суде файла были подлинными, корректными с точки зрения целостности, а письмо отправили пакетными средствами, однако, на наш взгляд, это было бы очень странное для вице-президента действие.)

Основные угрозы целостности

Из приведенного случая можно сделать вывод не только об *угрозах* нарушения целостности, но и об опасности слепого доверия компьютерной информации. Заголовки электронного письма могут быть подделаны; письмо в целом может быть фальсифицировано лицом, знающим пароль отправителя (мы приводили соответствующие примеры). Отметим, что последнее возможно даже тогда, когда целостность контролируется криптографическими средствами. Здесь имеет место взаимодействие разных аспектов информационной безопасности: если нарушена конфиденциальность, может пострадать целостность.

Основные угрозы целостности

Еще один урок: *угрозой* целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить *"неотказуемость"*, компьютерные данные не могут рассматриваться в качестве доказательства. Потенциально *уязвимы* с точки зрения нарушения **целостности** не только **данные**, но и **программы**. Внедрение рассмотренного выше *вредоносного ПО* - пример подобного нарушения.

Основные угрозы целостности

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, *кража*, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

Основные угрозы конфиденциальности

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, *угрозы* ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

Основные угрозы конфиденциальности

Многим людям приходится выступать в качестве пользователей не одной, а целого ряда систем (информационных сервисов). Если для доступа к таким системам используются многоразовые пароли или иная конфиденциальная информация, то наверняка эти данные будут храниться не только в голове, но и в записной книжке или на листках бумаги, которые пользователь часто оставляет на рабочем столе, а то и попросту теряет. И дело здесь не в неорганизованности людей, а в изначальной непригодности парольной схемы.

Основные угрозы конфиденциальности

Невозможно помнить много разных паролей; рекомендации по их регулярной (по возможности - частой) смене только усугубляют положение, заставляя применять несложные схемы чередования или вообще стараться свести дело к двум-трем легко запоминаемым (и столь же легко угадываемым) паролям.

Основные угрозы конфиденциальности

Описанный класс *уязвимых* мест можно назвать размещением конфиденциальных данных в среде, где им не обеспечена (зачастую - и не может быть обеспечена) необходимая защита. *Угроза* же состоит в том, что кто-то не откажется узнать секреты, которые сами просятся в руки. Помимо паролей, хранящихся в записных книжках пользователей, в этот класс попадает передача конфиденциальных данных в открытом виде (в разговоре, в письме, по сети), которая делает возможным *перехват данных*. Для *атаки* могут использоваться разные технические средства (подслушивание или прослушивание разговоров, пассивное прослушивание сети и т.п.), но идея одна - осуществить доступ к данным в тот момент, когда они наименее защищены.

Основные угрозы конфиденциальности

Угрозу перехвата данных следует принимать во внимание не только при начальном конфигурировании ИС, но и, что очень важно, при всех изменениях. Весьма опасной *угрозой* являются... выставки, на которые многие организации, недолго думая, отправляют оборудование из производственной сети, со всеми хранящимися на них данными. Остаются прежними пароли, при удаленном доступе они продолжают передаваться в открытом виде. Это плохо даже в пределах защищенной сети организации; в объединенной сети выставки - это слишком суровое испытание честности всех участников.

Основные угрозы конфиденциальности

Еще один пример изменения, о котором часто забывают, - хранение данных на резервных носителях. Для защиты данных на основных носителях применяются развитые системы управления доступом; копии же нередко просто лежат в шкафах и получить доступ к ним могут многие.

Основные угрозы конфиденциальности

Перехват данных - очень серьезная *угроза*, и если конфиденциальность действительно является критичной, а данные передаются по многим каналам, их защита может оказаться весьма сложной и дорогостоящей. Технические средства перехвата хорошо проработаны, доступны, просты в эксплуатации, а установить их, например на кабельную сеть, может кто угодно, так что эту *угрозу* нужно принимать во внимание по отношению не только к внешним, но и к внутренним коммуникациям.

Основные угрозы конфиденциальности

Кражи оборудования являются *угрозой* не только для резервных носителей, но и для компьютеров, особенно портативных. Часто ноутбуки оставляют без присмотра на работе или в автомобиле, иногда просто теряют. Опасной нетехнической *угрозой* конфиденциальности являются *методы морально-психологического воздействия*, такие как ***маскарад*** - выполнение действий под видом лица, обладающего полномочиями для доступа к данным (см., например, статью Айрэ Винклера "Задание: шпионаж" в Jet Info, 1996, 19).

Основные угрозы конфиденциальности

К неприятным *угрозам*, от которых трудно защищаться, можно отнести ***злоупотребление полномочиями***. На многих типах систем привилегированный пользователь (например системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример - нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Таковы основные *угрозы*, которые наносят наибольший ущерб субъектам информационных отношений.